120

AF/3621

PATENT APPLICATION
Attorney's Do. No. 8514-58

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of: Ned HOFFMAN

Serial No. 09/639,948 Examiner: Firmin BACKER

Filed: August 17, 2000 Group Art Unit: 3621

For: SYSTEM AND METHOD FOR TOKENLESS BIOMETRIC AUTHORIZATION OF ELECTRONIC COMMUNICATIONS

TRANSMITTAL LETTER

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Enclosed for filing in the above-referenced application are the following:

- ☒ Appellant's Brief (in Support of Appeal), in triplicate
- ☒ Exhibit "A"
- ☒ Exhibit "B"
- ☒ PTO Form 2038 authorizing credit card payment in the amount of $165.00 for the above-listed fee
- ☒ Any deficiency or overpayment should be charged or credited to deposit account number 13-1703. A duplicate copy of this sheet is enclosed.

Customer No. 20575

Respectfully submitted,

MARGER JOHNSON & McCOLLOM, P.C.

Ariel S. Rogson, Reg. No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
1030 SW Morrison Street
Portland, OR 97205
503-222-3613

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450
Date: April 12, 2004
Ariel S. Rogson

Attorney's Doc. No. 8514-58

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Ned HOFFMAN

Serial No.: 09/639,948 Group Art Unit: 3621

Filed: August 17, 2000 Examiner: Firmin BACKER

For: **SYSTEM AND METHOD FOR TOKENLESS BIOMETRIC AUTHORIZATION OF ELECTRONIC COMMUNICATIONS**

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S BRIEF UNDER 37 C.F.R. § 1.192

Appeal is taken from the Examiner's Office Action mailed November 10, 2003 finally rejecting claims 1-67 in this application.

This Appeal Brief is further to the Notice of Appeal mailed in this case on February 10, 2004.

The fees required under §1.17(c) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This Brief is transmitted in triplicate.

This Brief contains these items under the following headings, and in the order set forth below.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST
37 C.F.R. § 1.192(c)(1)

Indivos Corporation is the real party in interest.

II. RELATED APPEALS AND INTERFERENCES
37 C.F.R. § 1.192(c)(2)

There are no other appeals or interferences known to Appellant, the Appellant's representative, or assignee that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS
37 C.F.R. § 1.192(c)(3)

Status of All the Claims:

1. Claims presented: 1-67
2. Claims withdrawn from consideration but not cancelled: NONE
3. Claims canceled: NONE
4. Claims pending: 1-67 of which:
   a. Claims allowed: NONE
   b. Claims rejected: 1-67

All the rejected claims, namely claims 1-67, are being appealed. The appealed claims are eligible for appeal, having been finally rejected.

IV. STATUS OF AMENDMENTS
37 C.F.R. § 1.192(c)(4)

On November 5, 2002, the Examiner issued an Office Action rejecting claims 1 to 63 as originally filed under 35 U.S.C. § 101 as claiming the same invention as that of claims 1 to

51 of copending Application No. 09/398,914. On January 31, 2003, Applicant responded to the Office Action by presenting the argument that claims in this case are drawn to materially different subject matter. Within this response, Applicant also amended claims 58, 60, 61, and 62 to correct the numbering of these claims to be 60, 61, 62, and 63, respectively.

On April 9, 2003, the Examiner issued a second Office Action presenting new grounds for rejection of claims 1 to 63 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,457,747 to Drexler et al. and objecting to claim 1 because of an informality within the claim. On August 20, 2003, Applicant responded to this Office Action by amending claim 1 to correct the informality, presenting the argument that the claims are not anticipated by Drexler et al., amending claims 1, 4, 5, 7, 32, 36, 37, and 39 to broaden the scope of these claims, and adding new claims 64 to 67. In response to this Amendment, on November 10, 2003, the Examiner issued a Final Office Action rejecting claims 1 to 67 under the new grounds of 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,457,747 to Drexler et al. in view of Mark Rechtin's article *Fingerprinting Technology Makes for Best ID System*, published by the Orange County Business Journal, May 14th, 1990.

V. SUMMARY OF THE INVENTION
37 C.F.R. § 1.192(c)(5)

Methods and systems for tokenless accessing, processing and presentation of electronic communications using a user's biometric are shown by exemplary independent claims 1 and 32. The methods involve tokenless authorization of an electronic communication which is achieved by identifying a user by comparing the user's bid biometric sample to biometric samples stored in a database and authorizing the electronic communication if the user is successfully identified. The systems comprise the devices and apparatuses that enable one to achieve the method of tokenless authorization of electronic communications through the use of biometric sampling. The systems and methods satisfy the need for a fraud-resistant way for users to universally access, process, and present their electronic communications without requiring a token such as a magnetic swipe card.

VI. ISSUES ON APPEAL
37 C.F.R. § 1.192(c)(6)

The Examiner has rejected claims 1-67 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,457,747 to Drexler et al. in view of Mark Rechtin's article *Fingerprinting Technology Makes for Best ID System*, published by the Orange County Business Journal, May 14th, 1990.

For the convenience of the Board of Appeals, the entire Office Action dated April 9, 2003 and the entire Final Rejection dated November 10, 2003 have been reproduced and attached as Exhibits 1 and 2, respectively. The Office Action dated November 5, 2002 is not attached because the Examiner has apparently accepted the traversal of the rejection under 35 U.S.C. § 101.

The issue before the Board of Appeals is whether these rejections should be reversed.

VII. GROUPING OF CLAIMS
37 C.F.R. § 1.192(c)(7)

The claims include eight groups of claims. Claims 1, 3, 8, 13, 14, 16, 27, 28, 32, 33, 35, 40, 45, 46, 48, 59, 60, 66 and 67 are grouped together. Claims 2, 34 and 61 are grouped together. Claims 4 and 36 are grouped together. Claims 5-7, 9, 15, 37-39, 41 and 47 are grouped together. Claims 17-25, 49-57, 62, 64 and 65 are grouped together. Claims 26, 29-31, 58 and 63 are grouped together. Claims 10, 12, 42 and 44 are grouped together. Claims 11 and 43 are grouped together.

VIII. ARGUMENT
37 C.F.R. § 1.192(c)(8)

In the non-final Office Action dated April 9, 2003, the Examiner rejected claims 1-63 under the grounds that these claims were anticipated by Drexler et al. under 35 U.S.C. § 102(e). The Examiner relied on Drexler as anticipating independent claims 1 and 32 and did not present a *prima facie* argument that Drexler anticipated claims 2-31 and 33-63. The Examiner simply stated that these claims disclose the same inventive concepts at claims 1 and 32. Claims 2-31 and 33-67 further define the inventions of claims 1 and 32, respectively, and these claims also add further limitations that distinguish claims 2-31 and 33-67 over claims 1 and 32, and therefore are not the same inventive concepts. The reasons why the claims are patentable are discussed below, first in general and then with specific reference to each group of claims.

A. The Examiner's Broad-brush Office Actions Disregarded Patentable Distinctions Between the Invention as Claimed and the Prior Art.

In an amendment filed on August 11, 2003, appellant responded with arguments that the current application is directed toward a method and system of tokenless biometric identification and authorization for use in various electronic communications. Appellant further argued that the entire method and system can be carried out without using smartcards

or magnetic stripe cards. Appellant noted that the most obvious difference from the cited art is that Drexler requires the use of a card, whereas the invention does not. In this response, Appellant also amended claims 1, 4, 5, 7, 32, 36, 37, and 39 to broaden those claims.

Even though the appellant had not amended claims to narrow them, in the Office Action dated November 10, 2003, the Examiner raised new grounds for rejection and made the action final. Specifically the Examiner stated that in response to the arguments presented with respect to the previous Office Action, the "arguments with respect to claims 1-67 have been considered but are moot in view of the new ground(s) of rejection."

The Examiner rejected claims 1-67 as obvious from Drexler in view of an article titled "Fingerprint Technology Makes for Best ID System," published by the Orange County Business Journal, May 14th, 1990, and authored by Mark Rechtin. The Examiner relied on Drexler as teaching all of the limitations of independent claims 1 and 32 except that Drexler fails to teach an inventive concept of an electronic communication that is biometrically-authorized without the user having to present smartcards or magnetic stripe cards. The Examiner relied on the Rechtin article as teaching this element missing from Drexler. As in the earlier Office Action dated April 9, 2003, the Examiner did not present a *prima facie* argument that claims 2-31 and 33-67 are obvious from Drexler in view of Rechtin. Once again, the Examiner simply stated that these claims disclose the same inventive concepts at claims 1 and 32.

On January 26, 2004, appellant filed an Amendment after Final in response to the Final Office Action. In this amendment, the appellant argued that it is not possible to adopt Drexler to take advantage of the teaching of Rechtin for several reasons, including that Drexler requires the use of a card to store the biometric sample. Appellant again argued that the Examiner did not indicate where the limitations of claims 2-31 and 33-67 are specifically taught within Drexler or Rechtin and that these claims add further inventive features that are patentable in their own right over the combination of Drexler and Rechtin.

On February 5, 2004, Ariel S. Rogson held an interview with the Examiner. The appellant pointed out that the amendments made in the Response to Office Action dated April 9, 2003, did not narrow the claims and therefore did not necessitate on their own the new grounds for rejection by the Examiner. The appellant again pointed out that the Examiner had yet to make a specific rejection of any of the dependent claims. The Examiner responded that the dependent claims 2-31 and 33-67 disclose the same inventive concept as independent claims 1 and 32.

In response to the appellant's amendment and interview the Examiner issued an Advisory Action dated February 20, 2004, rejecting the request for reconsideration and indicating that the appellant's argument was not persuasive.

B. The Claimed Subject Matter Has Substantial Patentable Differences Over the Prior Art.

Claims 1-67 are improperly rejected under 35 U.S.C. § 103(a). Independent claim 1 is directed toward a method for tokenless biometric authorization. A user electronically submits a registration biometric sample. The registration biometric sample is electronically transmitted via a public communications network. The registration biometric sample is then stored in a master electronic identicator. The user then submits a bid biometric sample, which is transmitted to an electronic identicator. The user is identified by comparing the bid biometric sample with at least one registration biometric sample. Upon successful identification, an electronic communication is authorized. The entire method can be carried out without using smartcards or magnetic stripe cards.

Independent claim 32 is directed toward a system for tokenless biometric authorization. The system includes a communication input apparatus, which includes a data entry device to form an electronic communication. A biometric input apparatus includes a device to scan a biometric sample from the user. A master electronic identicator includes a database to store biometric samples from registered users and a comparator to compare received biometric samples with previously stored biometric samples. The system also includes a public network to transmit data between the biometric input apparatus and the master electronic identicator and an electronic communication authorization to authorize execution of a communication upon successful identification of the user. The system can operate without using smartcards or magnetic stripe cards.

In contrast, Drexler teaches a system for deterring fraudulent use of cards. The user has a card, which stores both the user's biometric sample and limits on the user of the card to obtain benefits. The user initially records his biometric sample on the card. Then, when the user presents the card to obtain services, the user provides another biometric sample, which is compared with the biometric data stored on the card. If the biometric sample matches the biometric data stored on the card, then the user limit data is accessed from the card, and if the use requested by the person is authorized, the user receives the desired benefits.

The Examiner acknowledged that Drexler fails to teach authorizing an electronic communication without using a smartcard or magnetic stripe card. The Examiner cited the Rechtin newspaper article as teaching this concept.

C. The Dependent Claims Add Further Substantial Patentable Distinctions.

Further in the appellant's application, claims 2, 34 and 61 are additionally directed generally toward an electronic identicator that can be a computer database remotely located from the user that stores registration biometric samples from registered users. Claims 4 and 36 are additionally directed generally toward both identification and authorization of a user utilizing a comparison of a bid biometric sample with a registered biometric sample. Claims 5-7, 9, 15, 37, 38, 39, 41, and 47 are additionally directed toward identifying both a third-party enterprise and a user for authorization of an electronic communication. Claims 17-19, 20-25, 49-57, 64, and 65 are additionally directed generally toward use of a rule-module that can be user customized wherein upon invocation of the rule-module after identification, an electronic communication is executed. Claims 26, 29-31, 58, and 63 are additionally directed generally toward further identifying a rule-module clearinghouse that can be a computer database for storing all or a subset of all of the users rule-modules. Claims 10, 12, 42, and 44 are additionally directed generally toward prevention of fraud when a user's registered biometric sample is determined to have been fraudulently duplicated. Claims 11 and 43 are additionally directed generally toward identification of a user attempting to re-register a biometric sample.

Now that the patent application and the cited art of Drexler and Rechtin have been discussed in general, the claims can be specifically discussed.

D. Each Group of Claims is Patentable Over Drexler in View of Rechtin.

1. The Claims of Group 1 Include Subject Matter Not Disclosed by Drexler or Rechtin.

The first group of claims consists of claims 1, 3, 8, 13, 14, 16, 27, 28, 32, 33, 35, 40, 45, 46, 48, 59, 60, 66 and 67, of which independent claim 1 is a representative member. Independent claim 32 is directed to a system supporting the method of claim 1. However, the arguments presented with respect to claim 1 also apply to claim 32. Claim 1 is patentable over the combination of Drexler and Rechtin. The Examiner stated that Drexler teaches a method for tokenless biometric authorization of an electronic communication. However,

Drexler teaches a system for deterring fraudulent use of cards and cards are precisely what the appellant's application is designed to eliminate.

In Drexler, the user has a card, which stores both the user's biometric sample and limits on the use of the card to obtain benefits. The user initially records his biometric sample on the card. Then, when the user presents the card to obtain services, the user provides another biometric sample, which is compared with the biometric data stored on the card. If the biometric sample matches the biometric data stored on the card, then the user limit data is accessed from the card, and if the use requested by the person is authorized, the user receives the desired benefits.

The Examiner acknowledged that Drexler fails to teach authorizing an electronic communication without using a smartcard or magnetic stripe card. The Examiner cited the Rechtin newspaper article as teaching this concept. The Examiner then concluded that it would be obvious to modify Drexler to take advantage of Rechtin.

It is not possible to adapt Drexler to take advantage of the teachings of Rechtin. There are several reasons why this is so. First, as noted in appellant's Response to the Office Action dated April 9, 2003, Drexler *relies* on the use of a card to store the biometric sample. Thus, Drexler teaches away from appellant's invention. A person of ordinary skill in the art would not think to combine Drexler, which teaches a system requiring a card, with Rechtin, which according to the Examiner suggests using biometrics without a card. The Examiner points to no motivation that could overcome the contradictions in this approach.

Second, Rechtin predates Drexler. Consequently, Drexler, at the time of his invention, had as part of the public knowledge the information described in Rechtin. But Drexler chose instead to design a system that uses a card, even though he constructively knew it had been suggested by Rechtin to design a biometric system that did not use a card. This suggests that Drexler himself, probably the person best qualified to indicate how his invention could be adapted, did not believe his invention could be modified to operate without a card.

Third, Rechtin does not provide an enabling description of any method or system employing the fingerprint comparison machines mentioned in the article. As a reference, Rechtin can only be cited for the concept of a cardless system. But because Rechtin does not enable one of ordinary skill in the art to implement this system, any other limitations of the claims must be found in Drexler for the claims to be obvious. This includes how a cardless system could be implemented. But Drexler does not disclose the necessary limitations to implement a cardless system.

Fourth, Rechtin quoted the research and development director of one company, stating that adoption of cardless biometric systems would be ubiquitous within 5-10 years of the publication date of Rechtin. As Rechtin was published in 1990, Rechtin expected cardless biometric systems to be "ubiquitous" by 2000. Yet here we are in 2004, still relying on non-biometric access control systems. Clearly, Rechtin and the supposed experts he quoted underestimated the complexity of biometric systems. This suggests that the modification of Drexler according to Rechtin is not as simple as the Examiner believes, and therefore not an obvious combination. The unfulfilled prophesies of Rechtin and the experts he cited in 1990 stand out as evidence of long-standing, unmet need – both indicia of non-obviousness.

Fifth, even if it were possible to modify Drexler according to the teaching of Rechtin (a position the appellant disputes), the claimed combination would not be obvious. As Drexler teaches a system that relies on a card, adapting Drexler to eliminate the card would require completely redesigning the system. For example, Drexler uses the card to identify the user, and then uses the biometric stored on the card to verify the user's identity. To eliminate the card as suggested by the Examiner would require introducing into Drexler some other way to identify the user, so that the biometrics can continue to be used to verify the user's identity. Applicant submits that the Examiner, in making the rejection, has employed impermissible hindsight.

Accordingly, the combination of Drexler and Rechtin does not teach or suggest a cardless system of user identification and authorization, and claim 1 is not obvious over Drexler in view of Rechtin. Similarly, claims 3, 8, 13, 14, 16, 27, 28, 32, 33, 35, 40, 45, 46, 48, 59, 60, 66 and 67 are allowable.

2. The Claims of Group 2 Add Further Distinguishing Features Over Drexler and Rechtin.

The second group of claims consists of claims 2, 34 and 61, of which claim 2 is a representative member. Claim 2 depends from claim 1 and is additionally directed toward storing registered biometric samples in a master electronic identicator, where that master electronic identicator includes a database of registration biometric samples from many users. The Examiner did not present any arguments specifically directed to claim 2. Drexler teaches storing the user's biometric sample on the card. Unless many people shared that user's card in Drexler (a wholly impractical idea), the card will only store the biometric data for one person. The Drexler card is not a database storing registration biometric samples from many

users and thus Drexler does not teach the concept of a master electronic identicator. Accordingly, claim 2 is patentable over Drexler in view of Rechtin. Similarly, claims 34 and 61 are allowable.

3. The Claims of Group 3 Add Further Distinguishing Features Over Drexler and Rechtin.

The third group of claims consists of claims 4 and 36, of which claim 4 is a representative member. Claim 4 depends from claim 1 and is additionally directed to using the electronic identicator to compare a user's bid biometric sample to a registration biometric sample to both identify the user and authorize an electronic communication without having to present smartcards or magnetic swipe cards. The Examiner again did not present any arguments specifically directed to claim 4. The Examiner might have been thinking that Drexler could be modified to use the biometric to identify the user, as claimed in appellant's invention. But such a modification would eliminate the need for Drexler. The appellant points out that the purpose of Drexler, *as stated in the title of Drexler*, is to provide a system to *verify* a user that avoids fraud as opposed to identification of the user. If biometrics were used to *identify* the user, there would be no concern about fraud. (Indeed, appellant's invention specifically addresses this issue.) Without a concern about fraud, Drexler becomes irrelevant. Thus, Drexler cannot be modified from a card-based system that uses biometrics to *verify* a user's identity into a cardless system that *identifies* a user.

Also, because the Drexler card stores only one user's biometric data, Drexler cannot perform user *identification*. Identification is the process of determining a user's identity. In effect, identification answers the question "Who am I?" Identification assumes that there is no information already suggesting the user's identity. In contrast, *verification* answers the question "Am I who I say I am?" Because there is only one user's biometric data stored on the Drexler card, the user has already identified himself, and is asking the system to *verify* his identity.

Another way to look at the difference between identification and verification is to consider what happens in the equipment performing the processes. In identification, the offered biometric sample is compared with at least a subset of the registered biometric samples, so that the system can say, "Of all the registered biometric samples I looked at, the offered biometric sample most likely matches this one." But in verification, the offered biometric sample is compared with *only one* registered biometric sample: the one associated with the person the user claims to be. The system says either "He is whom he says he is," or

"He is not whom he says he is." The system makes no effort to compare the offered biometric sample with any other registered biometric sample to determine the user's true identity.

To give yet another explanation of the difference between identification and verification, consider the situation where a person is attempting to commit fraud and assert that he is someone else. (Note that avoiding fraud is the stated purpose of Drexler, both in the title and technical field of Drexler.) Drexler would compare the offered biometric sample of the criminal with that of the card, and determine that they do not match. Drexler would then deny the criminal the benefits he sought. In contrast, appellant's invention would identify the criminal (assuming the criminal has registered with the system, without which he could not use the system). This means that the police could be sent to arrest the criminal knowing his identity. Drexler cannot accomplish this, because Drexler does not perform identification.

Drexler mentions a library, which stores biometric information. But, as described at column 8, lines 7-27, Drexler uses the library only to re-verify the user's identity as an anti-fraud measure, and not for identification. Because Drexler does not teach biometric identification, Drexler in combination with Rechtin cannot make claim 4 obvious. Similarly, claim 36 is likewise patentable.

4. The Claims of Group 4 Add Further Distinguishing Features Over Drexler and Rechtin.

The fourth group of claims consists of claims 5-7, 9, 15, 37-39, 41 and 47, of which claim 5 is a representative member. Claim 5 depends from claim 1 and is additionally directed toward a third-party enterprise submitting registration identity data and that registration identity data being used to identify a third-party enterprise in conjunction with a user being biometrically identified and an electronic communication biometrically authorized without the user having to present smartcards or magnetic swipe cards. The Examiner again did not present any arguments specifically directed to claim 5. As the appellant explained in the specification at page 6, lines 21-31 and page 7, lines 1-20, there exists a problem of enterprise communication centers being overwhelmed by the increase in electronic communications. Appellant's invention provides a computerized electronic communications system that can simultaneously accommodate a user's need to universally access, process and present electronic communications with optimal convenience and increase the accuracy,

speed and cost-effectiveness of the handling of these electronic communications by enterprise communication centers.

Neither Drexler nor Rechtin make any mention of incorporating the identification of enterprise operations in addition to the identification and authorization of a user's electronic communication. Accordingly, claim 5 is patentable over Drexler in view of Rechtin. Similarly, claim 6, 7, 9, 15, 37-39, 41 and 47 are allowable.

5. The Claims of Group 5 Add Further Distinguishing Features Over Drexler and Rechtin.

The fifth group of claims consists of claims 17-25, 49-57, 62, 64 and 65, of which claims 17 and 18 are representative members. Claim 17 depends from claim 1 and is additionally directed toward utilization of rule module formation and invocation steps where the rule-module includes at least one user-customized pattern data associated with at least one execution command. As further recited in claim 18, the data pattern could be any of a number of data including a unique user identification code, demographic information, digital signature or data on user behavior patterns (as well as many other recited possibilities). Again, the Examiner did not present any arguments specifically directed at claim 17. Neither Drexler nor Rechtin include rule-modules. Drexler is specifically directed toward preventing fraudulent use of a card and does not mention any additional rule-module features. Accordingly, claims 17 and 18 are patentable over Drexler in view of Rechtin. Similarly, claims 19-25, 49-57, 62, 64 and 65 are allowable.

6. The Claims of Group 6 Add Further Distinguishing Features Over Drexler and Rechtin.

The sixth group of claims consists of claims 26, 29-31, 58 and 63, of which claim 26 is a representative member. This claim is directed further toward using a master rule-module clearinghouse for storing the rule-modules of many users. Again, the Examiner did not present any arguments specifically directed at claim 26. As described above, Drexler mentions a library, which stores biometric information and not rule-module information. As described at column 8, lines 7-27, Drexler uses the library only to re-verify the user's identity as an anti-fraud measure, and not for the storing of many users' rule-modules. Accordingly, claim 26 is patentable over Drexler in view of Rechtin. Similarly, claims 29-31, 58 and 63 are allowable.

7. The Claims of Group 7 Add Further Distinguishing Features Over Drexler and Rechtin.

The seventh group of claims consists of claims 10, 12, 42 and 44, of which claims 10 and 12 are representative members. These claims are directed toward a user providing a personal identification code and that personal identification code being changed when the user's registered biometric sample is determined to have been fraudulently duplicated. Again, the Examiner presented no arguments specifically directed at claims 10 and 12. At column 8, lines 5-22, Drexler describes a mismatch in biometric information resulting in a denial of authorization and possible apprehension. Drexler also mentions mismatches resulting from replacement cards but also describes the result as a denial of authorization and possible apprehension. Appellant's invention requires a personal identification code and affirmatively changes that code when the registered sample has been fraudulently duplicated. Drexler does not disclose the use of a personal identification and fails to disclose any responses to detected fraudulent tampering of the registered biometric sample on the Drexler card or in the Drexler library. Accordingly, claims 10 and 12 are patentable over Drexler in view of Rechtin. Similarly, claims 42 and 44 are also allowable.

8. The Claims of Group 8 Add Further Distinguishing Features Over Drexler and Rechtin.

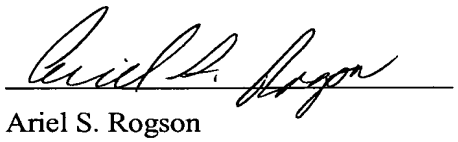
The eighth grouping of claims consists of claims 11 and 43 of which claim 11 is a representative member. Claim 11 is patentable over the combination of Drexler and Rechtin. The claim is additionally directed to alerting the electronic identicator of claim 1 that a user has attempted to re-register a biometric sample. Once again, the Examiner did not present any arguments directed specifically at claim 11. Drexler lacks any disclosure directed toward identifying a user that has attempted to re-register a biometric sample. Accordingly, claim 11 is patentable over Drexler in view of Rechtin. Similarly, claim 43 is also allowable.

In summary, because Drexler fails to teach authorizing an electronic communication without using a smartcard or magnetic stripe card, because it is not possible to adapt Drexler to take advantage of any teachings in Rechtin, and because Drexler and Rechtin fail to disclose many of the distinctly patentable features of the dependent claims, the rejection of claims 1-67 based on the combination of Drexler and Rechtin is inappropriate.

CONCLUSION

For the foregoing reasons, Appellant requests that the Board reverse the Examiner's rejections to Appellant's claims.

Respectfully submitted,
MARGER JOHNSON & MCCOLLOM, P.C.



Ariel S. Rogson
Registration No. 43,054

MARGER JOHNSON & McCOLLOM, P.C.
1030 S.W. Morrison Street
Portland, Oregon 97205
(503) 222-3613

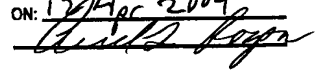
I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO:

☐ COMMISSIONER OF PATENTS AND TRADEMARKS WASHINGTON D.C. 20231

☒ MAIL STOP Appeal Brief - Patents
COMMISSIONER FOR PATENTS
BOX 1450
ALEXANDRIA, VA 22313-1450

☐ BOX _____
COMMISSIONER
FOR TRADEMARKS 2900 CRYSTAL DRIVE ARLINGTON, VA 22202-3513

ON: 17 Dec 2004



APPENDIX
37 C.F.R. § 1.192(c)(9)

The text of the claims on appeal (1-67) is:

1. A method for tokenless biometric authorization of an electronic communication, using a biometric sample, a master electronic identicator, and a public communications network, wherein said method comprises:

a. an electronic communication formation step, wherein at least one communication comprising electronic data is formed;

b. a user registration step, wherein a user electronically submits a registration biometric sample taken directly from a person of the user;

c. a public network data transmittal step, wherein the registration biometric sample is electronically transmitted to a master electronic identicator via a public communications network, said master electronic identicator comprising a computer database which electronically stores all of the registration biometric samples from all of the registered users;

d. a user registration biometric storage step, wherein the registration biometric sample is electronically stored within the master electronic identicator;

e. a bid biometric transmittal step, wherein a bid biometric sample, taken directly from the person of the user, is electronically transmitted to at least one electronic identicator;

f. a user identification step, wherein an electronic identicator compares the bid biometric sample to at least one registration biometric sample previously stored in an electronic identicator, for producing either a successful or failed identification of the user;

g. an electronic communication authorization step, wherein upon a successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic stripe cards.

2. The method of claim 1 wherein during the bid biometric transmittal step, the electronic identicator comprises any of the following: a master electronic identicator, and; a subset electronic identicator, said subset electronic identicator comprising a computer database which electronically stores a subset of all of the registration biometric samples from registered users.

3. The method of claim 1 wherein any steps of said method occur in any of the following chronological sequences: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

4. The method of claim 1, further comprising:

a. a first comparison step, wherein a subset electronic identicator compares the bid biometric sample taken directly from the person of the user with at least one registration biometric sample previously stored in the subset electronic identicator for producing either a successful or failed identification of the user;

b. a public network data transmittal step, wherein if the subset electronic identicator returns a failed identification result, the bid biometric sample is electronically transmitted via a public communications network to a master electronic identicator;

c. a second comparison step, wherein a master electronic identicator compares the bid biometric sample to at least one registration biometric sample previously stored in the master electronic identicator for producing either a successful or failed identification of the user;

d. a communication authorization step, wherein upon the earliest successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic swipe cards.

5. The method of claim 1 further comprising:

a. an enterprise registration step, wherein an enterprise electronically submits registration identity data;

b. a public network data transmittal step, wherein the enterprise registration identity data is electronically transmitted to a master electronic identicator via a public communications network;

c. an enterprise registration identity data storage step, wherein the enterprise registration identity data is electronically stored within the master electronic identicator;

d. an enterprise bid identity data network transmittal step, wherein enterprise bid identity data is electronically transmitted to at least one electronic identicator, said electronic identicator comprising any of the following: a subset electronic identicator and a master electronic identicator;

e. an enterprise identification step, wherein an electronic identicator compares the enterprise bid identity data with enterprise registration identity data previously stored in the electronic identicator, for producing either a successful or failed identification of the enterprise;

f. an electronic communication authorization step, wherein upon a successful identification of the enterprise by an electronic identicator and a successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic swipe cards.

6. The method of claim 5 wherein any steps of said method occur in any of the following chronologies: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

7. The method of claim 5 further comprising:

a. a first comparison step, wherein a subset electronic identicator compares the enterprise bid identity data with enterprise registration identity data previously stored in the subset electronic identicator for producing either a successful or failed identification of the enterprise;

b. a public network data transmittal step, wherein if the subset electronic identicator returns a failed identification result, the enterprise bid identity data is electronically transmitted via a public communications network to a master electronic identicator;

c. a second comparison step, wherein a master electronic identicator compares the enterprise bid identity data with enterprise registration identity data previously stored in the master electronic identicator for producing either a successful or failed identification of the enterprise;

d. a communication authorization step, wherein upon the earliest successful identification of the user by an electronic identicator and the earliest successful identification of the enterprise by an electronic identicator, at least one electronic communication is authorized for execution;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic swipe cards.

8. The method of claim 1 wherein the biometric sample taken directly from the person of the user comprises any of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

9. The method of claim 5 wherein the enterprise is a legally formed entity comprising any of the following: a corporation, a foundation, a non-profit organization, a sole proprietorship, a limited liability company, and a partnership.

10. The method of claim 1 wherein during the user identification step, the user provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

11. The method of claim 1 further comprising a user re-registration check step, wherein the user's registration biometric sample is compared by at least one electronic identicator to previously registered biometric samples wherein if a match occurs, the electronic identicator is alerted to the fact that the user has attempted to re-register.

12. The method of claim 10 further comprising a biometric theft resolution step, wherein a user's personal identification code is changed when the user's registered biometric sample is determined to have been fraudulently duplicated.

13. The method of claim 1, wherein an electronic communication comprises any of the following: an email communication, a telephone call, an encrypted data packet, an Internet telephony communication, and a facsimile.

14. The method of claim 1, wherein during the communication authorization step, any of the following is used: an intranet, an extranet, a local area network, a wide area network, a cable network, a wireless network, a telephone network, the Internet, an ATM network, or an X.25.

15. The method of claim 5 wherein enterprise registration identity data comprises any of the following: an alpha-numeric code, a hardware identification code, an email address, a financial account, a biometric of an authorized enterprise representative, a non-

financial data repository account, a telephone number, a mailing address, a digital certificate, a network credential, an Internet protocol address, a digital signature, an encryption key, and an instant messaging address.

16. The method of claim 1 wherein the communication authorization step further comprises a third-party communications step, wherein the electronic identicator electronically communicates with a third-party server in order to authorize the electronic communication.

17. The method of claim 1 further comprising:

a. a rule-module formation step, wherein a rule-module is formed in an electronic clearinghouse, said rule-module further comprising at least one user-customized pattern data which is associated with at least one execution command;

b. a rule-module invocation step, wherein upon a successful identification of the user, at least one previously designated user-customized rule-module is invoked;

c. an electronic communication execution step, wherein upon the invocation of a user-customized rule-module, at least one electronic communication is executed.

18. The method of claim 17 wherein pattern data comprises any of the following: a user unique identification code: demographic information; an email address; a financial account; a biometric; internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature.

19. The method of claim 17 wherein said execution commands further comprise user-customized instructions for executing any of the following: accessing of stored electronic data, processing of electronic data, and presentation of electronic data.

20. The method of claim 19 wherein user-customized accessing of stored electronic data further comprises execution of any of the following: activating of an Internet-

connected device; accessing of a secured physical space, and unlocking of a secured physical device.

21. The method of claim 19, wherein user-customized processing of electronic data further comprises invoking any of the following: a digital certificate, an identity scrambler, a database authorization field, an electronic consumer loyalty or consumer rewards incentive, an electronic advertisement, an instant messaging program, real-time tracking of an incoming caller or an email sender, a time and attendance monitoring program, an emergency home alarm and personal safety notification program, a real-time challenge-response program, a call-center queuing prioritization program, a call-center routing prioritization program, an email-center queuing prioritization program, an email-center routing prioritization program, an automated caller or emailer response program, a call-forwarding program, and an electronic intelligent software program for electronic data search and retrieval.

22. The method of claim 19 wherein user-customized presentation of electronic data comprises any of the following: a print-out, a computer screen display, an audio message, a tactile sensation and a holographic image.

23. The method of claim 17 wherein the rule-module invocation step further comprises a third-party communications step, wherein the electronic rule-module clearinghouse communicates with one or more third-party computers in order to invoke a rule-module.

24. The method of claim 17, wherein user-customized pattern data is provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic identicator, the electronic rule-module clearinghouse, and a user-authorized third party.

25. The method of claim 17, wherein user-customized execution commands are provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic rule-module clearinghouse, the electronic identicator and a user-authorized third party.

26. The method of claim 17 further comprising:

a. a master rule-module storage step, wherein all of the rule-modules from all of the registered users are stored in a master rule-module clearinghouse ;

b. a subset rule-module storage step, wherein a subset of all of the rule-modules from registered users is stored in a subset rule-module clearinghouse;

c. a rule-module invocation step, wherein upon a successful identification of the user, at least one user-customized rule-module is invoked by any of the following: a subset rule-module clearinghouse and a master rule-module clearinghouse;

d. an electronic communication execution step, wherein upon the invocation of a user-customized rule-module, at least one electronic communication is executed.

27. The method of claim 1 wherein during the registration biometric network transmittal step, any of the following public networks is used: a cable network, a wireless cellular network, a wireless digital network, a telephone network, a wide area network, the Internet, an ATM network, and an X.25 connection.

28. The method of claim 1 wherein during the public network data transmittal step, any of the following networks is used: a cable network, a wireless cellular network, a wireless digital network, a telephone network, a wide area network, the Internet, an ATM network, and an X.25 connection.

29. The method of claim 26 further comprising:

a. a first rule-module invocation step, wherein the subset rule-module clearinghouse attempts to invoke at least one user-customized rule-module;

b. a public network data transmittal step, wherein if the subset rule-module clearinghouse fails to invoke a user-customized rule-module, the request is transmitted to a master rule-module clearinghouse via a public communications network;

c. a second rule-module invocation step, wherein a master rule-module clearinghouse attempts to invoke at least one user-customized rule-module;

d. an electronic communication execution step, wherein upon the earliest invocation of a user-customized rule-module, at least one electronic communication is executed.

30. The method of claim 26 wherein the master rule-module clearinghouse comprises a computer database which electronically stores all of the rule-modules for all of the registered users.

31. The method of claim 26 wherein the subset rule-module clearinghouse comprising a computer database which electronically stores a subset of all of the rule-modules for registered users.

32. A system for tokenless biometric authorization of an electronic communication, using an electronic communication input apparatus, a biometric input apparatus, and a master electronic identicator, wherein said system comprises:

a. a communication input apparatus, further comprising a data entry device for formation of an electronic communication;

b. a biometric input apparatus, further comprising a device for electronically scanning a biometric sample directly from a person of a user;

c. at least one master electronic identicator, further comprising:

i) a computer database containing all of the electronically stored biometric samples from all of the registered users;

ii) a comparator that electronically compares a received biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user;

d. a data transmittal public network that electronically transmits data between the biometric input apparatus and a master electronic identicator;

e. an electronic communication authorization platform that authorizes execution of at least one electronic communication upon a successful identification of the user by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic stripe cards.

33. The device of claim 32 wherein the master electronic identicator further comprises a computer database which: has a location which is physically remote from the site at which the user submits a biometric sample directly from his person, and; requires the use of a public communication network that enables receipt of an electronically transmitted registration biometric sample.

34. The device of claim 32 further comprising a subset electronic identicator having: a computer database containing a subset of all stored biometric samples from registered users in the computer system, and; a comparator that compares a received biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user.

35. The device of claim 32 wherein any component of said system is used in any of the following chronological sequences: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

36. The device of claim 34, further comprising:

a. a first comparator, comprising a subset electronic identicator comparator that compares the bid biometric sample taken directly from the person of the user with at least one registration biometric sample previously stored in the subset electronic identicator for producing either a successful or failed identification of the user;

b. a data transmittal public network, comprising a public communications network that electronically transmits data between the subset electronic identicator and a master electronic identicator;

c. a second comparator, comprising a master electronic identicator comparator which, if the subset electronic identicator fails to successfully identify the user, compares the bid biometric sample to at least one registration biometric sample previously stored in the master electronic identicator for producing either a successful or failed identification of the user;

d. a communication authorization platform, that authorizes execution of an electronic communication upon the earliest successful identification of the user by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic swipe cards.

37. The device of claim 34 further comprising:

a. an enterprise data input apparatus for an enterprise to electronically input registration identity data;

b. a data transmittal public network, further comprising a public communications network that electronically transmits data between the enterprise data input apparatus and a master electronic identicator;

c. an electronic communication authorization platform, that authorizes execution of an electronic communication upon a successful identification of the enterprise by an electronic identicator and a successful identification of the user by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic swipe cards.

38. The device of claim 37 wherein any component is used in any of the following chronological sequences: simultaneously, and; separated by any increment of time including seconds, minutes, hours, days, weeks, months, and years.

39. The device of claim 37 further comprising:

a. a first comparator, comprising a subset electronic identicator comparator that compares the enterprise bid identity data with enterprise registration identity data previously stored in the subset electronic identicator for producing either a successful or failed identification of the enterprise;

b. a data transmittal public network, further comprising a public communications network that electronically transmits data between the subset electronic identicator and a master electronic identicator;

c. a second comparator, comprising a master electronic identicator comparator which, if the subset electronic identicator fails to successfully identify the enterprise, compares the enterprise bid identity data with enterprise registration identity data previously stored in the master electronic identicator for producing either a successful or failed identification of the enterprise;

d. a communication authorization platform, that authorizes execution of an electronic upon the earliest successful identification of the user by an electronic identicator and the earliest identification of the enterprise by an electronic identicator;

wherein an electronic communication is biometrically-authorized without the user having to present smartcards or magnetic swipe cards.

40. The device of claim 32 wherein the biometric sample taken directly from the person of the user comprises any of the following: a fingerprint, a facial scan, a retinal image, an iris scan, and a voice print.

41. The device of claim 37 wherein the enterprise is a legally formed entity comprising any of the following: a corporation, a foundation, a non-profit organization, a sole proprietorship, a limited liability company, and a partnership.

42. The device of claim 32 wherein the user further provides a personal identification code to the electronic identicator along with a bid biometric sample for purposes of identifying the user.

43. The device of claim 37 further comprising a user re-registration platform, wherein the user's registration biometric sample is compared by at least one electronic identicator to previously registered biometric samples wherein if a match occurs, the electronic identicator is alerted to the fact that the user has attempted to re-register.

44. The device of claim 42 further comprising a biometric theft resolution platform, wherein a user's personal identification code is changed when the user's registered biometric sample is determined to have been fraudulently duplicated.

45. The device of claim 32, wherein an electronic communication comprises any of the following: an email, a telephone call, an encrypted data packet, an Internet telephony, and a facsimile.

46. The device of claim 32, wherein the data transmittal public network further comprises any of the following: an extranet, a wide area network, a cable network, a wireless network, a telephone network, the Internet, an ATM network, or an X.25.

47. The device of claim 37 wherein enterprise registration identity data comprises any of the following: an alpha-numeric code, a hardware identification code, an email address, a financial account, a biometric of an authorized enterprise representative, a non-financial data repository account, a telephone number, a mailing address, a digital certificate,

a network credential, an Internet protocol address, a digital signature, an encryption key, and an instant messaging address.

48. The device of claim 32 further comprising a third-party server interconnecting network, wherein the electronic communication execution platform interconnects with one or more third-party servers in order to execute the electronic communication.

49. The device of claim 32 further comprising:

a. a rule-module clearinghouse, further comprising at least one user-customized pattern data which is associated with at least one execution command;

b. a rule-module invocation platform, that invokes at least one previously designated user-customized rule-module upon successful identification of the user;

c. an electronic communication execution platform, that executes at least one electronic communication upon the invocation of a user-customized rule-module.

50. The device of claim 49 wherein pattern data comprises any of the following: a user unique identification code: demographic information; an email address; a financial account; a biometric; internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature.

51. The device of claim 49 wherein said execution commands further comprise user-customized instructions for execution of any of the following: accessing of stored electronic data, processing of electronic data, and presentation of electronic data.

52. The device of claim 51 wherein user-customized accessing of stored electronic data further comprises execution of any of the following: activation of an Internet-connected device; accessing of a secured physical space, and unlocking of a secured physical device.

53. The device of claim 51, wherein user-customized processing of electronic data further comprises invoking any of the following: a digital certificate, an identity scrambler, a database authorization field, an electronic consumer loyalty or consumer rewards incentive, an electronic advertisement, an instant messaging program, real-time tracking of an incoming caller or an email sender, a time and attendance monitoring program, an emergency home alarm and personal safety notification program, a real-time challenge-response program, a call-center queuing prioritization program, a call-center routing prioritization program, an email-center queuing prioritization program, an email-center routing prioritization program, an automated caller or emailer response program, a call-forwarding program, and an electronic intelligent software program for electronic data search and retrieval.

54. The device of claim 51 wherein user-customized presentation of electronic data comprises any of the following: a print-out, a computer screen display, an audio message, a tactile sensation and a holographic image.

55. The device of claim 49 wherein the rule-module invocation platform is interconnected with one or more third-party computers.

56. The device of claim 49, wherein user-customized pattern data is provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic identicator, the electronic rule-module clearinghouse, and a user-authorized third party.

57. The device of claim 49, wherein user-customized execution commands are provided to the electronic rule-module clearinghouse by any of the following: the user, the electronic rule-module clearinghouse, the electronic identicator and a user-authorized third party.

58. The device of claim 49 further comprising:

a. a master rule-module clearinghouse, comprising a computer database storing all of the rule-modules for all of the registered users;

b. a subset rule-module clearinghouse, comprising computer database storing a subset of all of the rule-modules for registered users;

c. a rule-module invocation platform, that invokes at least one user-customized rule-module upon identification of the user, said platform comprising any of the following: a subset rule-module clearinghouse and a master rule-module clearinghouse;

d. an electronic communication execution platform, that executes at least one electronic communication upon the invocation of a user-customized rule-module.

59. The device of claim 32 wherein the data transmittal public network further comprises: a cable network, a wireless cellular network, a wireless digital network, a telephone network, a wide area network, the Internet, an ATM network, and an X.25 connection.

60. The device of claim 32 wherein the master electronic identicator further comprises a computer database having a location which is physically remote from the site at which the user submitted the registration biometric sample.

61. The device of claim 34 wherein the subset electronic identicator further comprises a computer database: being physically remote from the master identicator, and; capable of using any communications network for receiving the bid biometric sample.

62. The device of claim 58 further comprising:
a first rule-module invocation platform, comprising a subset rule-module clearinghouse that invokes at least one user-customized rule-module;
a data transmittal public network, wherein if the subset rule-module clearinghouse fails to invoke a user-customized rule-module, the request is transmitted via a public communications network to a master rule-module clearinghouse;
a second rule-module invocation platform, comprising a master rule-module clearinghouse that invokes at least one user-customized rule-module;
an electronic communication execution platform, that executes at least one electronic communication upon the earliest invocation of a user-customized rule-module by a rule-module clearinghouse.

63. The device of claim 58 wherein the subset rule-module clearinghouse is physically remote from the master rule-module clearinghouse.

64. The method of claim 21 wherein pattern data comprises any of the following: a user unique identification code: demographic information; an email address; a financial account; a biometric; internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature.

65. The device of claim 53 wherein pattern data comprises any of the following: a user unique identification code: demographic information; an email address; a financial account; a biometric; internet browsing patterns; a non-financial data repository account; a telephone number; a mailing address; purchasing patterns; database authorization fields; financial credit report data; a call-center queuing, routing and automated response program; an email-center queuing, routing and automated response program; data on pre-paid accounts or memberships for products or services; electronic data utilization patterns; employee status; job title; data on user behavior patterns; a digital certificate; a network credential; an internet protocol address; a digital signature; an encryption key; an instant messaging address; user-customized medical records; an electronic audio signature; and an electronic visual signature.

66. The method of claim 1 wherein:

the user registration step includes the user electronically submitting a personal identification code;

the public network data transmittal step includes electronically transmitting the personal identification code to a master electronic identicator via a public communications network, said master electronic identicator comprising a computer database which electronically stores all of the registration biometric samples and personal identification codes from all of the registered users;

the user registration biometric storage step includes electronically storing the registration biometric sample within the master electronic identicator associated with the personal identification code;

the bid biometric transmittal step includes electronically transmitting to at least one electronic identicator the personal identification code of the user; and

the user identification step includes the electronic identicator comparing the bid biometric sample to at least one registration biometric sample associated with the personal identification code previously stored in an electronic identicator, for producing either a successful or failed identification of the user.

67. The device of claim 32 wherein:

the system further comprises means for receiving a personal identification code coupled to the biometric input apparatus;

the computer database contains all of the electronically stored biometric samples and associated personal identification codes from all of the registered users; and

the comparator electronically compares the received biometric sample with previously stored biometric samples associated with the personal identification code to deliver either a successful or failed identification of the user.

Exhibit "A"

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/639,948	08/17/2000	Ned Hoffman	STA-25 8514-58	4850

20575 7590 04/09/2003

MARGER JOHNSON & MCCOLLOM PC
1030 SW MORRISON STREET
PORTLAND, OR 97205

EXAMINER	
BACKER, FIRMIN	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 04/09/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	Applicant(s)	
09/639,948	HOFFMAN, NED	
Examiner	**Art Unit**	
Firmin Backer	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2003* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-63* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Response to Request for Reconsideration

This is in response to a request for reconsideration file January 31st, 2003. Claims 1-63 are being reconsidered in this action.

Response to Arguments

1. Applicant's arguments with respect to claims 1-63 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

2. Claim 1 is objected to because of the following informalities: Applicant discloses "*the person*" in line 11. Applicant is advised to replace "*the*" by "*a*" in order to overcome examiner's objection.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-63 are rejected under 35 U.S.C. 102(e) as being anticipated by Drexler (U.S. Patent 5,457,747).

5. As per claim 1, Drexler et al. teach a method for tokenless biometric authorization of an electronic communication, using a biometric sample, a master electronic identicator, and a public communications network, wherein said method comprises an electronic communication formation step, wherein at least one communication comprising electronic data is formed, a user registration step, wherein a user electronically submits a registration biometric sample taken directly from the person of the user, a public network data transmittal step, wherein the registration biometric sample is electronically transmitted to a master electronic identicator via a public communications network, said master electronic identicator comprising a computer database which electronically stores all of the registration biometric samples from all of the registered users, a user registration biometric storage step, wherein the registration biometric sample is electronically stored within the master electronic identicator, a bid biometric transmittal step, wherein a bid biometric sample, taken directly from the person of the user, is electronically transmitted to at least one electronic identicator, a user identification step, wherein an electronic identicator compares the bid biometric sample to at least one registration biometric sample previously stored in an electronic identicator, for producing either a successful or failed identification of the user, an electronic communication authorization step, wherein upon a successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution, wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory

tokens such as smartcards, or magnetic stripe cards (*see abstract, fig 1, 3, column 2 lines 30-3 line 36, 4 line 61-5 line 41).*

6. As per claim 32, Drexler et al. teach a system for tokenless biometric authorization of an electronic communication, using an electronic communication input apparatus, a biometric input apparatus, and a master electronic identicator, wherein said system comprises a communication input apparatus, further comprising a data entry device for formation of an electronic communication, a biometric input apparatus, further comprising a device for electronically scanning a biometric sample directly from the person of a user, at least one master electronic identicator, further comprising a computer database containing all of the electronically stored biometric samples from all of the registered users, a comparator that electronically compares received a biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user, a data transmittal public network that electronically transmits data between the biometric input apparatus and a master electronic identicator, an electronic communication authorization platform that authorizes execution of at least one electronic communication upon a successful identification of the user by an electronic identicator, wherein an electronic communication is biometrically-authorized without the user having to present any personalized man-made memory tokens such as smartcards, or magnetic stripe cards(*see abstract, fig 1, 3, column 2 lines 30-3 line 36, 4 line 61-5 line 41).*

7. As per claims 2-31 and 33-63, they disclose the same inventive concept as claim 1 and 32, therefore, they are rejected under the same rationale.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (*see form 892*).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 8:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 305-7687 for regular communications and (703) 305-7687 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

Firmin Backer
April 2, 2003

Notice of References Cited

Application/Control No.	Applicant(s)/Patent Under Reexamination	
09/639,948	HOFFMAN, NED	
Examiner	Art Unit	Page 1 of 1
Firmin Backer	3621	

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,229,764	07-1993	Matchett et al.	340/5.52
	B	US-5,457,747	10-1995	Drexler et al.	713/186
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

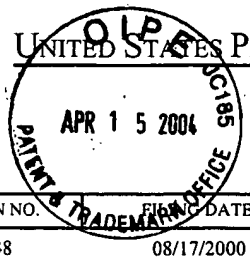
NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Exhibit "B"

UNITED STATES PATENT AND TRADEMARK OFFICE



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/639,948	08/17/2000	Ned Hoffman	STA-25	4850

9514-58

20575 7590 11/10/2003

MARGER JOHNSON & MCCOLLOM PC
1030 SW MORRISON STREET
PORTLAND, OR 97205

2/1/04 SD

EXAMINER	
BACKER, FIRMIN	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 11/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/639,948	HOFFMAN, NED	
	Examiner	Art Unit	
	Firmin Backer	3621	

-- Th MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for R ply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 August 2003* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-67* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-67* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

Response to Amendment

This is in response to an amendment file on August 20th, 2003 for letter for patent filed on August 17th, 2000 in which claims 1-64 were presented for examination. In the amendment, claims 1, 4, 5, 7, 32, 36, and 39 have been amended, no claim have been canceled, and claims 65-67 have been added. Claims 1-67 are pending in the letter.

Response to Arguments

1. Applicant's arguments with respect to claims 1-67 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Drexler et al (U.S. Patent no. 5,457,747) in view of Mark Rechtin (*Fingerprint Technology Makes for Best ID System, Published by Orange County Business Journal, May 14th, 1990*).

4. As per claim 1, Drexler et al teach a method for tokenless biometric authorization of an electronic communication, using a biometric sample, a master electronic identicator, and a public communications network, wherein the method comprises an electronic communication formation, wherein at least one communication comprising electronic data is formed a user registration step, wherein a user electronically submits a registration biometric sample taken directly from the person of the user, a public network data transmittal, wherein the registration biometric sample is electronically transmitted to a master electronic identicator via a public communications network, said master electronic identicator comprising a computer database which electronically stores all of the registration biometric samples from all of the registered users, s user registration biometric storage, wherein the registration biometric sample is electronically stored within the master electronic identicator, a bid biometric transmittal, wherein a bid biometric sample, taken directly from the person of the user, is electronically transmitted to at least one electronic identicator, a user identification, wherein an electronic identicator compares the bid biometric sample to at least one registration biometric sample previously stored in an electronic identicator, for producing either a successful or failed identification of the user, an electronic communication authorization wherein upon a successful identification of the user by an electronic identicator, at least one electronic communication is authorized for execution (*see abstract, figs 1 and 3, column 2 lines 20-3 lie 36, 4 lines 61-5 line 4)* . Drexel et al fail to teach an inventive concept of an electronic communication is biometrically-authorized without the user having to present smartcards, or magnetic stripe cards. However, Rechtin teaches an inventive concept of an electronic communication is biometrically-authorized without the user having to present smartcards, or magnetic stripe cards *(see abstract).* However, it would have

been obvious to one of ordinary skill in the art at time the invention was made to modify the inventive to include Rechtin's inventive concept of an electronic communication is biometrically-authorized without the user having to present smartcards, or magnetic stripe cards because this would have facilitate customer interaction with the secure transaction system.

5. As per claim 1, Drexler et al teach a system for tokenless biometric authorization of an electronic communication, using an electronic communication input apparatus, a biometric input apparatus, and a master electronic identicator, wherein said system comprises a communication input apparatus, further comprising a data entry device for formation of an electronic communication, a biometric input apparatus, further comprising a device for electronically scanning a biometric sample directly from the person of a user, at least one master electronic identicator, further comprising a computer database containing all of the electronically stored biometric samples from all of the registered users, a comparator that electronically compares received a biometric sample with previously stored biometric samples to deliver either a successful or failed identification of the user, a data transmittal public network that electronically transmits data between the biometric input apparatus and a master electronic identicator, an electronic communication authorization platform that authorizes execution of at least one electronic communication upon a successful identification of the user by an electronic identicator (*see abstract, figs 1 and 3, column 2 lines 20-3 lie 36, 4 lines 61-5 line 4)* . Drexel et al fail to teach an inventive concept of an electronic communication is biometrically-authorized without the user having to present smartcards, or magnetic stripe cards. However, Rechtin teaches an inventive concept of an electronic communication is biometrically-authorized without the user

having to present smartcards, or magnetic stripe cards (*see abstract).* However, it would have been obvious to one of ordinary skill in the art at time the invention was made to modify the inventive to include Rechtin's inventive concept of an electronic communication is biometrically-authorized without the user having to present smartcards, or magnetic stripe cards because this would have facilitate customer interaction with the secure transaction system.

6. As per claims 2-31 and 33-67, they are dependent upon claims 1 and 32 and disclose the same inventive concept as claims 1 and 32. Therefore, they are rejected under the same rationale

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firmin Backer whose telephone number is (703) 305-0624. The examiner can normally be reached on Mon-Thu 9:00 AM - 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James Trammell can be reached on (703) 305-9768. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 308-1113.

Firmin Backer
Examiner
Art Unit 3621

October 27, 2003

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Notice of References Cited

Application/Control No.	Applicant(s)/Patent Under Reexamination	
09/639,948	HOFFMAN, NED	
Examiner	Art Unit	Page 1 of 1
Firmin Backer	3621	

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Rechtin, Mark, Fingerprint Technology Makes for Best ID system, May 1990, Orange County Business Journal, NewPort Beach, Vol. 12, iss. 51, Sec. 1, page 7
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.